RSAC | 2025 Conference

Many Voices.
One Community.

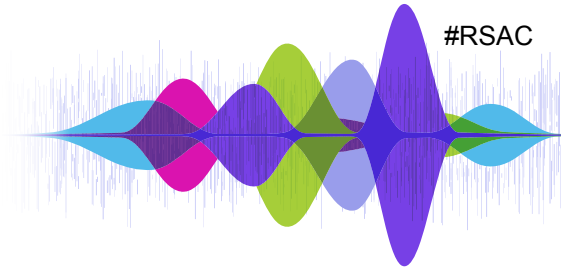
SESSION ID: CLS-W09

Beyond the CSRB Report: Critical Cloud Lessons for Today and Tomorrow

2:25pm/14h25', April 30, 2025, PDT or UTC -0700

Shin Adachi, CISSP, CCSP, CISM, CISA, PMP

PGP Key ID: 0x9F6E079A
Fingerprint: 758B D3AE 14B1 38AA A902 7A62
Independent Cybersecurity Consultant, Santa Clara, CA
https://www.linkedin.com/in/shin1adachi/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

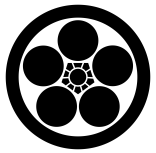
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

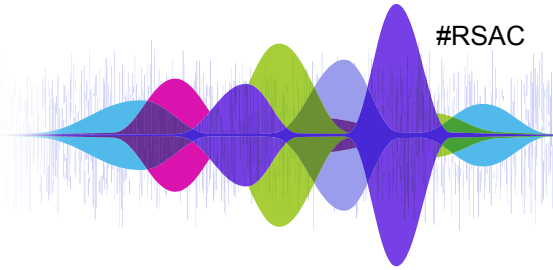
This presentation represents only personal views and opinions of the presenter, NOT the the opinion(s) or position(s) of any others including but not limited to my customers, and/or associations.

All trademarks and other intellectual properties are the properties of their respective owners.

The presenter is just a reader of the CSRB report and have no relationships with CSRB or any authors of this report.



How did this journey start?😅



Date: Fri, 31 Jan 2025 16:48:22 +0000

Subject: RSAC 2025 Conference - Upcoming Deadlines Reminder

Hi Shin,

I wanted to reach out and congratulate you again on being selected as a Speaker at RSAC™ 2025 Conference, taking place April 28-May 1 at the Moscone Center in San Francisco.

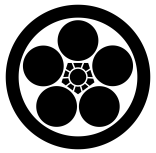
There are some important tasks that require your attention now and in the upcoming weeks. You can find more information on any of the tasks by visiting your.…

You can access … here: <URL here>

…

Speaker Manager, <A company name here>

On behalf of RSAC



Topic today

Homeland Security

Topics | News | In Focus | How Do I? | Get Involved | About DHS

Home » News » Press Releases » Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023

News
- All DHS News
- Apps
- Blog
- Comunicados de Prensa
- Data
- Events
- Fact Sheets
- Featured News
- Homeland Security LIVE
- Media Contacts

Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023

Release Date: April 2, 2024

WASHINGTON – Today, the U.S. Department of Homeland Security (DHS) released the Cyber Safety Review Board's (CSRB) findings and recommendations following its independent review of the Summer 2023 Microsoft Exchange Online intrusion. The review detailed operational and strategic decisions that led to the intrusion and recommended specific practices for industry and government to implement to ensure an intrusion of this magnitude does not happen again. Secretary of Homeland Security Alejandro N. Mayorkas received the CSRB report from the Board and delivered it to President Biden. This is the third review completed by the CSRB since the Board was announced in February 2022.

"Individuals and organizations across the country rely on cloud services every day, and the security of this technology has never been more important," **said Secretary Mayorkas**. "Nation-state actors continue to grow

Source: Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023: April 2, 2024 <https://www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer>

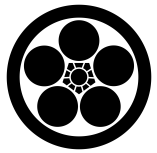
Review of the Summer 2023 Microsoft Exchange Online Intrusion

March 20, 2024
Cyber Safety Review Board

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

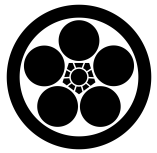
Why this report?

- Real Incident with a large scale (of impacts and victims)
  - Assessed as a persistent and sophisticated attack
- More Details inside a Cloud Service Provider than ever
- Details incident responses by different stakeholders
  - Victims
  - Cloud Service Provider
  - Authorities such as Intelligence, Law Enforcement, and Government agencies



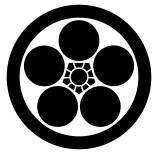
Why this report? (Continued)

- Lessons for different stakeholders
  - Incident Responders
  - Decision Makers
  - CSPs
  - Government Officials
  - Auditors
  - Corporate Communications, Government relations, and more



Agenda

- Incident Overview - What happened?
- Incident Responses by Different stakeholders:
  - Victims
  - Cloud Service Provider
- Unknowns
- Implications after the incident
- Lessons



RSAC | 2025 Conference

Incident Overview - What happened?

- Incident Responses by Different stakeholders:
  - Victims
  - Cloud Service Provider
- Unknowns
- Implications after the incident
- Lessons

Many Voices.
One Community.

Incident Overview

- Compromised Microsoft Exchange Online mailboxes
  - 22 Organizations including U.S. Departments of Commerce and State
    - including government agencies and three think tanks
    - including senior U.S. government representatives at that time working on National Security such as:
      - Commerce Secretary
      - US Ambassador to the PRC 🇨🇳
      - Assistant Secretary of State for East Asian and Pacific Affairs
      - A Congressman
- Right before State Secretary's visit to Beijing from June 18~19, 2023

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>
Reference: Secretary Blinken's Visit to the People's Republic of China (PRC) <https://www.state.gov/secretary-blinkens-visit-to-the-peoples-republic-of-china-prc/>

Incident Overview

- Compromised Microsoft Exchange Online mailboxes (Continued)
  - 22 Organizations including U.S. Departments of Commerce and State (Continued)
  - The non-U.S. victims included:
    - four (4) foreign government entities
    - three (3) private sector organizations
    - four (4) educational entities (page 8)
  - 500+ individuals around the world
    - Many of whom were linked to entities associated with Western European, APAC, Latin American, and Middle Eastern countries

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Overview

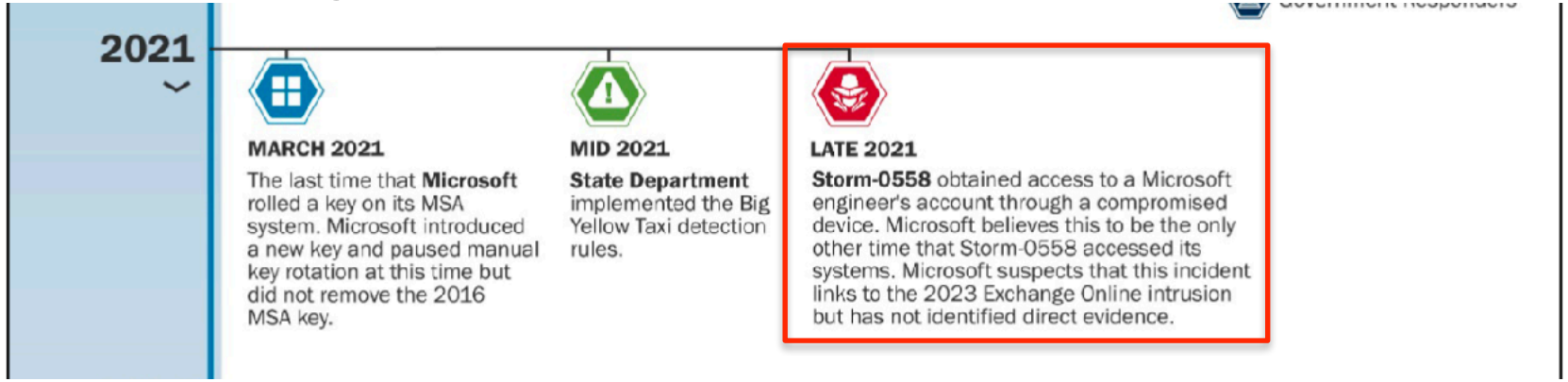
- by Storm-0558, assessed to be affiliated with PRC🇨🇳 for espionage
- by Authentication tokens signed by a Microsoft Services Account (MSA) signing key Microsoft had created in 2016
- This intrusion was found by the State Department SOC on June 15, 2023, before their Cloud Service Provider.

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Overview/Timeline

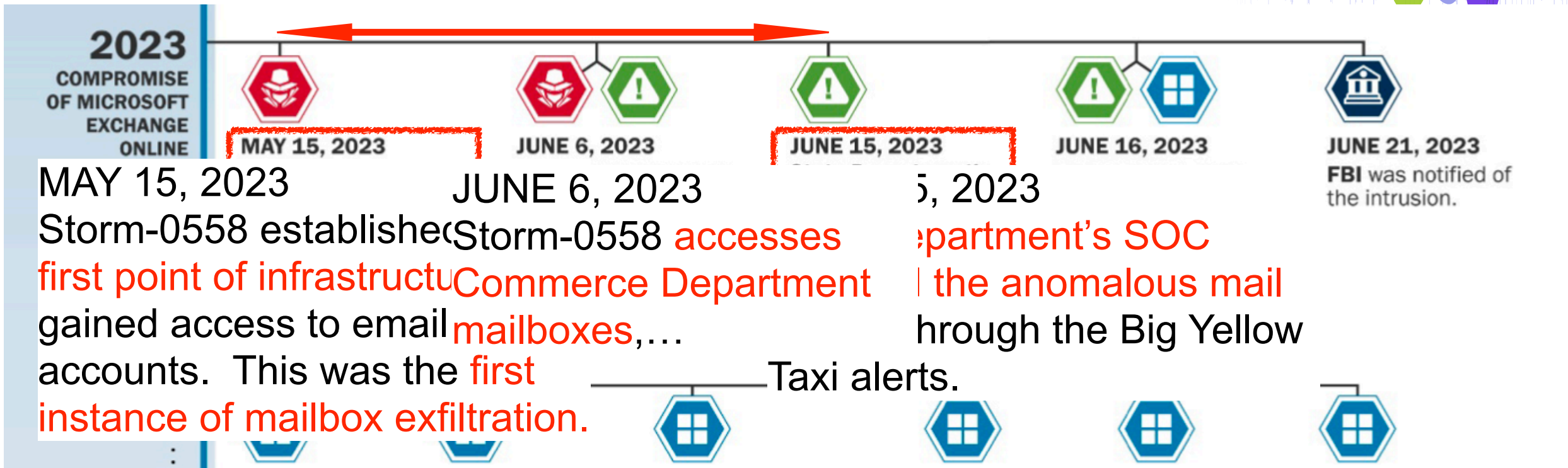
LATE 2021

Storm-0558 obtained access to a Microsoft engineer's account through a compromised device. Microsoft believes this to be the only other time that Storm-0558 access its systems. Microsoft suspects that this incident links to the 2023 Exchange Online Intrusion but has not identified direct evidence.


2021
MARCH 2021
The last time that Microsoft rolled a key on its MSA system. Microsoft introduced a new key and paused manual key rotation at this time but did not remove the 2016 MSA key.
MID 2021
State Department implemented the Big Yellow Taxi detection rules.
LATE 2021
Storm-0558 obtained access to a Microsoft engineer's account through a compromised device. Microsoft believes this to be the only other time that Storm-0558 accessed its systems. Microsoft suspects that this incident links to the 2023 Exchange Online intrusion but has not identified direct evidence.

Source: Appendix B: Microsoft Exchange Online Intrusion Timeline, Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Overview/Timeline



- **Before State Secretary's visit to Beijing from June 18~19, 2023**
  - "State's SOC had limited visibility into the activity but, based on the particular email accounts that the threat actor accessed, quickly determined that the targeted individuals were supporting the Secretary's upcoming trip to Beijing." (Page 10) 14

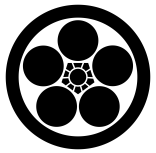
Source: Appendix B, Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Overview/ Adversary profile

- Storm-0558
  - Operates as its own distinct group
  - Information collection for PRC's intel needs
  - A possible link to Operation Aurora in 2009 and RSA SecurID token seed breach in 2011

In short, professional sniper or assassin for many of us

Source: Section 1.2.2 on Page 4, Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

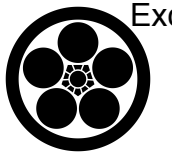


Incident Overview/ CSRB Recommendations

- CSRB Recommendations at a glance

1	MSFT CEO and BoDs to focus on Security Culture	9	Mergers and Acquisitions (M&A)
2	MSFT to deprioritize developments before security improvements	10	CSPs to define and adopt minimum standard for default audit logging
3	CSPs accountable for security outcomes of customers	11	CSPs to implement emerging standards for security
4	CSPs to stop charging security related logging	12~13	Standards bodies and CSPs to update standards for Identity Systems
5	CSPs to have logging and forensic capabilities	14~17	CSPs transparency to USG
6	Identity and credential management as a top priority for CSPs	18~20	Victim notification process to be developed
7	CISA to validate CSPs for USG annually	21~24	FedRAMP
8	Update cloud based identity systems in NIST SP 800-53	25	NIST to update security and privacy controls

Source: Table developed by the presenter from the Section 2 Finding and Recommendations (Page 17~24) of the Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>



RSAC | 2025 Conference

- Incident Overview- What happened?

Incident Responses by Different stakeholders:

- **Victims**
- Cloud Service Provider
  - Unknowns
  - Implications after the incident
  - Lessons

Incident Response by victims/ DETECTION

- Department of State SOC
- Thursday June 15, 2024
  - State Department's SOC observed multiple security alerts from their "Big Yellow Taxi", own custom detection rules to analyze MailItemsAccessed log
- Friday, June 16, 2024
  - State Department Security Team contacted their Cloud Service Provider
- They opened its investigation and confirmed Storm-0558 had gained access to certain user emails through State's OWA.
- 21 additional organizations and 503 related users were identified impacted by the attack.

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by victims/ How_Detected?

Why could the Department of State SOC detect the incident?

- Enhanced Logging as well as Basic one
- SOC investigated anomalies and confirmed the alert indicated malicious activity regardless of false positive Big Yellow Taxi detections in the past.
- Big Yellow Taxi, their own tool analyzed enhanced and basic logs including voluminous MailItemAccessed log
  - The report says:
    - “Just purchasing the additional logging alone would not have been enough; in fact, the Board heard that few organizations analyzed the voluminous MailItemsAccessed log in detail..”
    - “CISA assessed that the threat actor could not avoid generating the MailItemsAccessed log data during the intrusion, which meant that it could detect similar future activity if it had the relevant logs.” (Page 12)

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by victims/ How_Detected?

Why could the Department of State SOC detect the incident? (Continued)

- Big Yellow Taxi, their own tool to analyze enhanced logs
  - Custom alerting capabilities based on three years of experience dealing with anomalous access to mailboxes
  - Curated log events including MailItemAccessed to enumerate all apps accessing mailboxes within its infrastructure
  - Designed to detect deviations comparing baseline interactions of apps with Exchange Online

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by victims/ COMMERCE

- Challenges at Department of Commerce Enterprise SOC (ESOC)
- No Enhanced Logs
- Commerce ESOC did not have Enhanced logging [*]
- Microsoft activated enhanced logging, HOWEVER NO PAST LOGS available before that!
- The report says “Although Microsoft activated enhanced logging for identified victims who did not have the appropriate license, Microsoft could not give historical logs to customers unless they already had the premium licenses at the time of the intrusion. Thus, customers could capture data from the time that Microsoft enabled additional logging capabilities but were unable to view past intrusion activity.”

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by victims/LOGs

- LOGs and Investment MATTER!:
  - Why could the Department of State SOC detect the incident?

	Department of State	Department of Commerce and many others
Own custom tool developed	Yes	No
Enhanced Logging from CSP	Yes	No
Basic Logging from CSP	Yes	Yes

Source: Table developed by the presenter based on the Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

RSAC | 2025 Conference

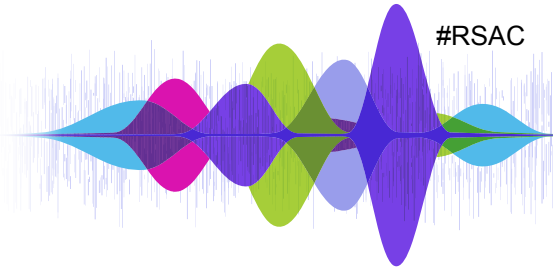
- Incident Overview- What happened?

Incident Responses by Different stakeholders:

- Victims
- **Cloud Service Provider**
  - Unknowns
  - Implications after the incident
  - Lessons

Many Voices.
One Community.

Incident Response by Cloud Service Provider

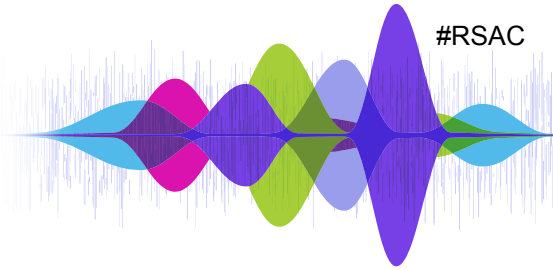


Challenges:

- The Customer, U.S. Department of State had found and notified the intrusion before the CSP.
- The CSP could not provide logs with more details during the incident for Department of Commerce because Commerce had not subscribed the enhanced log service before the incident and CSP didn’t have it anymore.

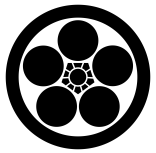
Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by Cloud Service Provider



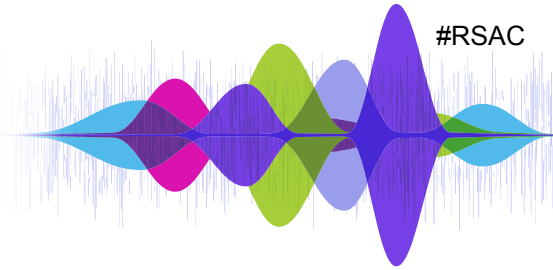
Challenges:

- A key was a key!
  - The signing key used for intrusions was issued by Microsoft in 2016 and revoked on June 24, 2023, after State Department detected the intrusion.
  - Although that key was supposed only for consumer OWA, it worked for Enterprise Exchange online as well.
  - No automated key rotation system for the Consumer MSA system, whole key rotation including manual process stopped in 2021



Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by Cloud Service Provider

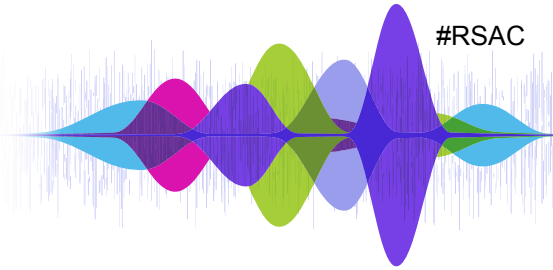


Challenges:

- CSRB assessed the stolen key also could have been used to compromise other Microsoft Cloud applications and Microsoft IDP reliant third-party applications. (Page 8)

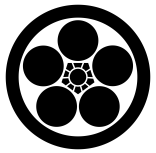
Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by Cloud Service Provider



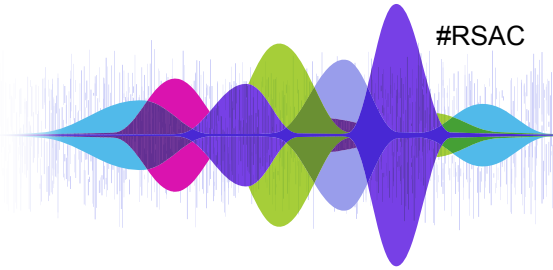
Challenges:

- Microsoft announced the acquisition of Affirmed Networks on March 26, 2020 and completed that on April 23, 2020.
- Microsoft believes Storm-0558 targeted an engineer of that company compromised the device prior to acquisition. Microsoft supplied corporate credentials to the acquired engineer, allowing the compromised device to access to Microsoft's corporate network and systems.
- Microsoft still could not explain how the Storm-0558 had obtained the 2016 key.



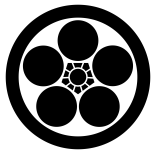
Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by Cloud Service Provider



Good:

- Microsoft had incident response, escalation procedures including preset urgency levels and emergency communication to most senior leadership including its Board of Directors, and cross team coordination for investigation upon notification from State Department.
- This allowed them to escalate from individual incident process to its Software and Services Incident Response Plan (SSIRP), then up to SEV-0, their highest urgency level.
- Cross team coordination assembled team members from their DART, MSTIC, and various security teams, resulting in their 46 hypotheses.



Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

RSAC | 2025 Conference

- Incident Overview- What happened?

Incident Responses by Different stakeholders:

- Victims
- Cloud Service Provider
- **Government authorities**
  - Unknowns
  - Implications after the incident
  - Lessons

Many Voices.
One Community.

Incident Response by Gov. Authorities

- NSA
  - Supported Department of State's response
- FBI
  - Shared details about the threat actor
  - Conducted an independent analysis on the disk image[*] and made its findings available to the broader group.
  - Victim coordination and notification with Microsoft (Section 1.3.3)
  - An example only LEAs could do: On June 21, 2023, after issuing a legal process to the U.S.-based VPS provider that hosted the attacker's infrastructure, the government obtained a disk image from the provider that contained valuable insights into the threat actor's intrusion

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Incident Response by Gov. Authorities

- CISA
  - Assisted Department of State's response
  - Assisted Department of Commerce's response
  - Conducted an independent analysis on the disk image and made its findings available to the broader group.
  - Tested to emulate the API used by the threat actor to exfiltrate email
  - Assessed that the threat actor could not avoid generating the MailItemsAccessed log data during the intrusion, which meant that it could detect similar future activity if it had the relevant logs.
  - Worked with International partners
  - Worked with Microsoft, the CSP

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

RSAC | 2025 Conference

- Incident Overview- What happened?
- Incident Responses by Different stakeholders:
  - Victims
  - Cloud Service Provider
  - Government Authorities

Unknowns
Implications
Lessons

Many Voices.
One Community.

Unknowns

- No sufficient logs available for Department of Commerce to learn what exactly happened during this intrusion.
- The CSP still could not explain how the Storm-0558 had obtained the signing key issued in 2016.

Source: Review of the Summer 2023 Microsoft Exchange Online Intrusion <https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf>

Implications: LOGs DO Matter!

PRESS RELEASE

CISA and Microsoft Partnership Expa Logging Capabilities Broadly

"Microsoft agreed to provide cloud security log features available to customers for free after enduring days of withering criticism following the state-linked email hacks against 25 of its customers, including the U.S. State

Released: July 19, 2023

many Microsoft customers will no logging capabilities at no addition

Access to New Logging by Default Will Enhance Cyber Defense and Incident Response

WASHINGTON – Based on a collaborative partnership between the Cybersecurity and Infrastructure Se customers will now have access to expanded cloud logging capabilities at no additional charge, which Microsoft's decision is a significant step toward advancing security by design principles and a strong ex cybersecurity at a national scale.

Source: <https://www.cybersecuritydive.com/news/microsoft-free-security-logs-Outlook-email-hack-backlash/688388/>
Source: <https://www.cisa.gov/news-events/news/cisa-and-microsoft-partnership-expands-access-logging-capabilities-broadly>

Microsoft offers free security logs amid backlash from State Department hack

Federal officials and rivals blasted the company for charging customers for additional security features.

Published July 19, 2023

David Jones
Reporter

Microsoft plans to save big by extending cloud server life, reducing capital expenditures. *Drew Angerer / Staff via Getty Images*

Microsoft agreed to provide cloud security log features available to customers for free, after enduring days of withering criticism following the state-linked email hacks against 25 of its customers, including the U.S. State Department.

The Cybersecurity and Infrastructure Security Agency announced the partnership with Microsoft to provide access to the cloud logging features by default Wednesday.

Implications: Sharing experience

ALERT

CISA Releases Microsoft Expanded Cloud Logs Implementation Playbook

Release Date: January 15, 2025

Today, CISA released the Microsoft Expanded Cloud Logs Implementation Playbook to help organizations get the most out of Microsoft's newly introduced logs in Microsoft Purview Audit (Standard). This step-by-step guide enables technical personnel to better detect and defend against advanced intrusion techniques by operationalizing expanded cloud logs.

The playbook details analytical methodologies tied to using these logs. Specifically, the playbook offers:

- An overview of the newly introduced logs in Microsoft Purview Audit (Standard) that enable organizations to conduct forensic and compliance investigations by accessing critical events (e.g., mail items accessed, mail items sent, and user searches in SharePoint Online and Exchange Online).
- A description of administration/enabling actions and ingestion of these logs to Microsoft Sentinel and Splunk Security Information and Event Management (SIEM) systems.
- A discussion of significant events in other M365 services, such as Teams.

Source: CISA Releases Microsoft Expanded Cloud Logs Implementation Playbook, January 15, 2025 <https://www.cisa.gov/news-events/alerts/2025/01/15/cisa-releases-microsoft-expanded-cloud-logs-implementation-playbook>

Implications: Sharing experience (continued)

PUBLICATION

Microsoft Expanded Cloud Logs Implementation Playbook

Enabling and operationalizing cloud logs to detect and defend against advanced intrusion techniques

Publish Date: January 15, 2025

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, IDENTITY THEFT AND PERSONAL CYBER THREATS, ORGANIZATIONS AND CYBER SAFETY

This playbook provides a detailed overview of the newly introduced logging capabilities in Microsoft Purview Audit (Standard). These capabilities enable organizations to conduct forensic and compliance investigations by accessing critical events, such as

- Mail items accessed,
- Mail items sent, and
- User searches in SharePoint Online and Exchange Online.

Source: Microsoft Expanded Cloud Logs Implementation Playbook, January 15, 2025
<https://www.cisa.gov/resources-tools/resources/microsoft-expanded-cloud-logs-implementation-playbook>
the document located at: <https://www.cisa.gov/sites/default/files/2025-01/microsoft-expanded-cloud-logs-implementation-playbook-508c.pdf>

Implications: Microsoft China

- "After a seven-month review, US federal regulators said in April that Microsoft needs to make "fundamental" reforms to its cybersecurity policies. The review board blamed Microsoft's corporate culture for a China-backed email hack, where Chinese hackers forged Microsoft authentication tokens to breach US government Outlook accounts." (PC Mag, July 8, 2024)

"Microsoft staff in China will also have to use Microsoft's Authenticator password manager and Identity Pass app on their iPhones for work to verify their identities in order to log into work devices, and Android access will be blocked." (PC Mag, July 8, 2024)

PC MAG Best Picks Reviews News How-To Find products, advice, tech news

PCMag editors select and review products independently. If you buy through affiliate links, we may earn commissions, which help support our testing.

PCMag UK > Software & Services > Games > Sony PlayStation Games > Computers & Electronics > Mobile Phones

Microsoft Employees in China Forced to Switch From Android to iPhones

Microsoft is telling its employees in China that they have to use company-supplied iPhone 15 devices for work going forward as part of its cybersecurity plans.

by Kate Irwin Jul 08, 2024

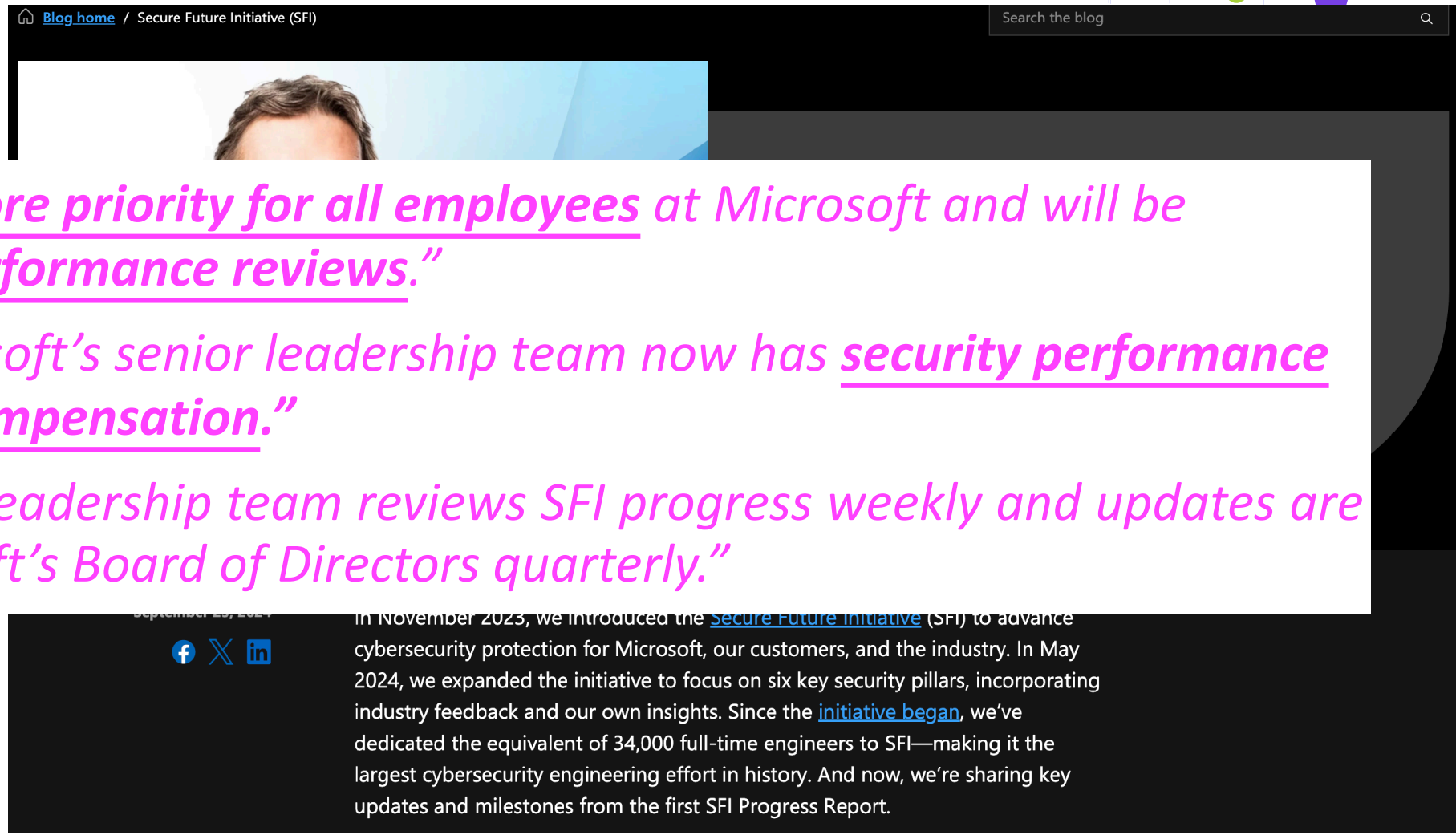
(Credit: Bloomberg/Contributor via Getty Images)

Microsoft is reportedly requiring all of its China-based employees to stop using Android phones for work purposes and switch to Apple iPhones for cybersecurity reasons. Microsoft staff in China will also have to use Microsoft's Authenticator password manager and Identity Pass app on their iPhones for work to verify their identities in order to log into work devices, and Android access will be blocked.

Microsoft notified the hundreds of impacted staff via an internal memo, Bloomberg reports Monday. The employees will each receive an iPhone 15 to use instead of Android smartphones

Sources:
<https://www.bloomberg.com/news/articles/2024-07-08/microsoft-orders-china-staff-to-switch-from-android-phones-to-iphones-for-work?le
<https://uk.pcmag.com/mobile-phones/153148/microsoft-employees-in-china-forced-to-switch-from-android-to-iphones>

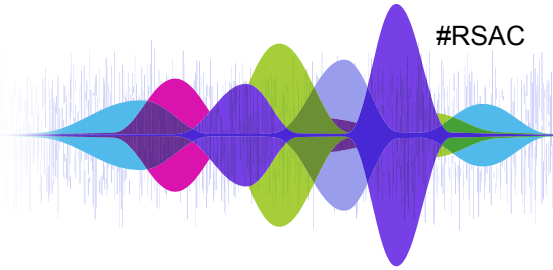
Implications:
Secure Future Initiative


Blog home / Secure Future Initiative (SFI)
Search the blog
In November 2023, we introduced the Secure Future Initiative (SFI) to advance cybersecurity protection for Microsoft, our customers, and the industry. In May 2024, we expanded the initiative to focus on six key security pillars, incorporating industry feedback and our own insights. Since the initiative began, we've dedicated the equivalent of 34,000 full-time engineers to SFI—making it the largest cybersecurity engineering effort in history. And now, we're sharing key updates and milestones from the first SFI Progress Report.

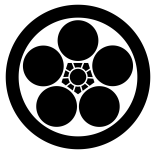
- *"Security is now **a core priority for all employees** at Microsoft and will be **included in their performance reviews**."*
- *"Additionally, Microsoft's senior leadership team now has **security performance directly linked to compensation**."*
- *"Microsoft's senior leadership team reviews SFI progress weekly and updates are provided to Microsoft's Board of Directors quarterly."*

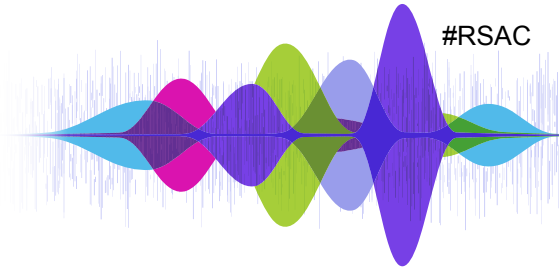
Source: <https://www.microsoft.com/en-us/security/blog/2024/09/23/securing-our-future-september-2024-progress-update-on-microsofts-secure-future-initiative-sfi/>

Lessons



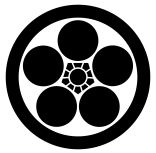
- Cloud? It's just someone else's computer.
- Clouds are not easy outsourcing for quick cost reduction.
  - Monitoring and Response
  - Development when necessary
  - Cloud Service Provider can't necessarily do all what we want.
  - Cloud Service Provider can be compromised as well.





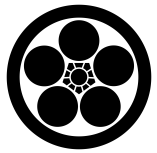
Lessons (continued)

- LOGs LOGs LOGs
  - Do we know what logs we need?
  - Can our Cloud Service Provider give us the logs we need timely?
- Monitoring and log analysis
  - How do you monitor the network and systems and analyze logs?
  - Logs without monitoring and analysis don’t help us.
- Identity and Access Management and Key Management
  - What if your key(s) and/or credential(s) are stolen for someone else to use?
  - How are your keys monitored and rotated?
- Are decision-makers fully aware of importance of **INVESTMENT?**

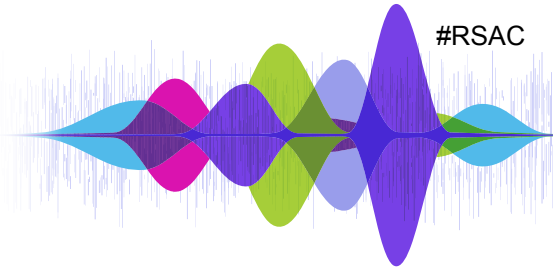


Lessons (continued)

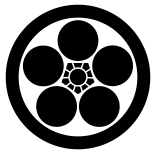
- after the “Closed” incident
  - “Closure” of incident may not mean the time for (my) vacation.
  - It may be the start of something new and bigger, as big as the whole organizational change from the top to the bottom.
  - A possible good example of how an incident could impact the whole organization after it was “closed”.



Lessons (continued)



- Updates existing practices, guidances, and policies:
  - Practices, guidances, and/or policies would need to be updated to reflect improvements and changes such as logs, identity managements, key managements, organizational changes, and changes at Cloud Service Providers.
- Review this CSRB report for more lessons for each of you
  - Each of us has different views, tasks, roles, experiences, and expertise!



Apply What You Have Learned Today

- Next week you should:
  - Start knowing ourselves: Check the status of ours, especially,
    - Keys and Key management
    - Everything around Digital identities, e.g. authentication, authorization, credentials, role based accesses
      - NIST SP800-63 Digital Identity Guidelines for your reference
    - How are LOGs managed? How are your systems monitored? What are monitored and analyzed (or not)?
    - Subscriptions and configurations of your cloud services
    - Audit reports in the past: What were audited and missed (depending on the scope) in the past audits?
    - Inventories: refer to the CIS (formerly SANS) Critical Security Controls
- In the first three months following this presentation you should:
  - Share your findings with stakeholders
    - Compile your findings in the first three months
    - Share the findings with IT and sysadmins, their management, and decision makers
- Within six months you should:
  - Track the progress
    - Inventory what were fixed or not yet
    - Confirm the target date of remaining fixes and ongoing challenges to fix them

Questions?

Source: illustAC

RSAC 2025 Conference

Many Voices.
One Community.

Thank you!

For more questions, inquiries, and feedback:

Shin Adachi, CISSP, CCSP, CISM, CISA, PMP
shin <a-t> adachi dot us
PGP Key ID: 0x9F6E079A
Fingerprint: 758B D3AE 14B1 38AA A902 7A62 D608 1CA7 9F6E 079A

@s_adachi

https://www.linkedin.com/in/shin1adachi/